WACS用户手册

安腾网络

2005-06-01

1. 简介和特性......3
1.1. 版本信息......3
1.2. 简介......3
1.3. 特性......3
2. WACS安装......5
3. WACS配置......5
3.1. 连接......5
3.2. 快速配置......7
3.3. 端口配置......9
3.3.1. WAN端口（E0 口）配置......9
3.3.2. LAN端口（E1 口）配置......10
3.3.3. DMZ端口（E2 口）配置......11
3.3.4. DHCP服务管理......12
3.4. 用户管理......13
3.4.1. 帐号管理......13
3.4.2. 在线用户......15
3.4.3. 导出数据......15
3.4.4. 导入数据......16
3.5. 认证管理......17
3.5.1. Radius管理......17
3.5.2. WEB认证管理......19
3.5.3. AP管理......21
3.6. 高级配置......22
3.6.1. 路由配置......22
3.6.2. NAT配置......23
3.6.3. ACL配置......24
3.6.4. ARP管理......25
3.6.5. Proxy ARP......26
3.7. 系统管理......26
3.7.1. 查看状态......27
3.7.2. 系统时间......27
3.7.3. 修改密码......28
3.7.4. 保存配置......28
3.7.5. 导出配置......29
3.7.6. 导入配置......30
3.7.7. 恢复出厂配置......30
3.7.8. 版本升级......31
3.7.9. 重新启动......32
4. 使用范例......32
4.1. AP作为认证点，WACS启用控制......32
4.2. AP作为认证点，WACS只启用认证服务......34
4.3. WACS作为认证点，启动WEB认证......34
5. 出厂配置主要内容......35

1. 简介和特性

1.1. 版本信息

本手册对应的正式版本信息为：WAS AOS 1.3。如果您手上的设备为旧版本或者更新的版本，请查看与版本对应的手册，或者联系本地的技术支持。

1.2. 简介

WACS 是用于对网络进行简单接入控制的系统，支持可以支持以太网，快速以太网或IEEE 802.11 无线网单独使用或者混合使用。

WACS 通过在Windows 98se/Me/2000/XP,Macintosh OS 9, Mac OS X (v10.1.5 or later), Linux, or Pocket PC 2000/2002运行标准的HTML浏览器（IE、Netscape Navigator）进行配置。

WACS 可以采用ADSL、LAN（Static IP）等方式接入Internet。WACS 可以提供通过交换机和无线AP为用户提供Internet接入，它通过对某些的特性的设置来控制受限制网络和非受限制网络的Internet接入。

1.3. 特性

- 可以建立利用 wacs 建立一个有线的或者无线 internet 接入，同时提供两个相对独立的局域网接入，以提供给您的员工和客户以及来访者使用。
- 把网络划分为 LAN 和 DMZ 两块，LAN 网络中的用户需要认证授权才能访问网络资源。
- 可以在本地管理 1024 个用户。
- 至少支持 200 个用户同时上网。
- 使用基于用户 ID/PASSWD 的认证和授权方式。

- 内置 RADIUS SERVER 提供本地认证功能。
- 支持 RADIUS 扩展认证方式。
- 支持本地 802.1X（EAP-MD5）方式认证。
- 支持 AP 作为 802.1X 认证点的认证方式。
- 内置 WEB SERVER，用户可以使用 WEB 认证。
- 可以定制用户的认证页面。
- 结合外置 RADIUS SERVER 可以提供详细的上网记录清单。
- 当认证点在 WACS 时，可以提供在线状态检测。
- 当认证点在 WACS 时，提供以 32Kbit 为步长的带宽控制
- 当认证点在 WACS 时，提供 Keep Alive 功能。
- 当认证点在 WACS 时，可以设置用户的闲置断线时间。
- 当认证点在 WACS 时，可以设置用户认证成功后出现的 URL。
- 支持 NAT。
- 可以使用静态 IP、PPPoE 客户端接入广域网。
- 内置 DHCP Server
- 内置高速策略路由引擎。
- 管理界面使用 WEB 方式。

2. WACS 安装

- 首先，请确认 WACS 没有连接电源，而且电源是关闭的。

- WAN接口（E0口）的连接

  用10/100BaseT连接线连接出口。出口可以是ADSL路由器的LAN口、cable modem的LAN口或者是企业内部互联网的交换端口。

- LAN端口（E1口）的接入

  企业网的交换机或者HUB用直连线连接用户电脑连接到上,另一端连到WACS的E1端口上。如果想将WACS直接与PC或无线AP连接上，请使用交叉线。

- DMZ端口（E2口）的接入

  企业网的交换机或者HUB用直连线连接用户电脑连接到上,另一端连到WACS的E2端口上。如果想将WACS直接与PC或无线AP连接上，请使用交叉线。

- 打开电源
- 检查指示灯，当有网络设备接入 WACS 对应端口的指示灯会亮

3. WACS 配置

可以通过浏览器对 WACS 进行远程配置。

进行配置的电脑需要：

- 基于 Windows, Macintosh, or Linux 操作系统，有以太网络适配器的电脑
- IE6 或者 Netscape Navigator　Version 6.0 或以上版本

3.1. 连接

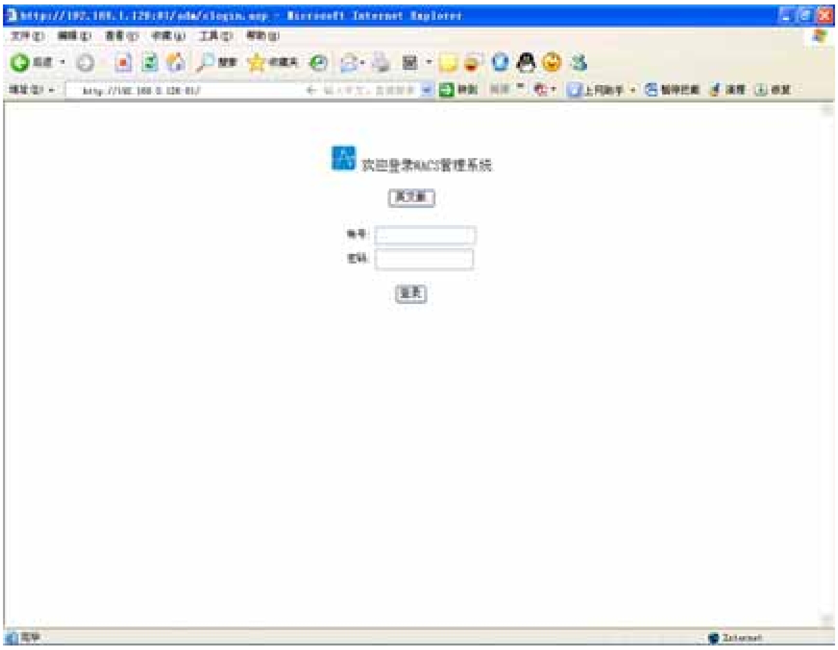
配置 WACS 时，请将你的管理电脑用网线连接在 WACS 的 WAN 端口（E0 口）网络端。

WACS 缺省的 E0 口地址为 192.168.0.126/255.255.255.0

- 配置你的电脑的 TCP/IP 配置设为 IP：192.168.0.x(1~254，除 126 外)；子网掩码：255.255.255.0；网关：192.168.0.126。

- 关掉使用代理服务器接入 internet 功能（以 win2000 为例）。请在控制面板>Internet 选项>连接>局域网设置中关掉代理服务器选项

打开IE浏览器；输入WACS管理地址http://192.168.0.126:81/，进入登陆界面（如下图）。使用admin作为管理员的登录，Username：:admin； Passwd：password；或者使用manager作为一般用户登录（仅具有查看权限），Username：:manager； Passwd：password。



登录成功后，进入管理界面，可以查看当前管理员，系统版本信息，系统启动，当前时间，以及系统的基本配置信息。如下图：

!! 注意：当改变任何配置时，请保存设置并重新启动 WACS!

3.2. 快速配置

建议第一次使用此设备，或者需要重新配置网络时，使用快速配置功能。

快速配置的步骤：

第一步：配置 WAN 口的地址

第二步：配置 LAN 和 DMZ 端口

LAN 为受限制端口（需要认证），DMZ 为非受限制端口（不需要认证）。

第三步：配置 DHCP 所用的 DNS 和 Web 认证等内容

本页内容除 DNS 外，都可以按照默认值填写。

按照快速配置的指引进行配置后，可以保证基本的网络通信。如果需要配置认证、用户等内容，请参看相关的部分。

3.3.端口配置

端口配置是对 WACS 的网络接口属性进行配置，包括 IP 地址、掩码、是否认证端口等。

3.3.1. WAN 端口（E0 口）配置

端口模式：配置 WAN 口的接入模式（静态 IP、PPPoE）

静态 IP 配置： IP 地址：输入 ISP 所提供的 IP 地址或者内部网络分配的地址；

子网掩码：输入 ISP 所提供的子网掩码或者内部网络的子网掩码；

默认网关：输入 ISP 所提供的网关的 IP 地址或者内部网络的网关。

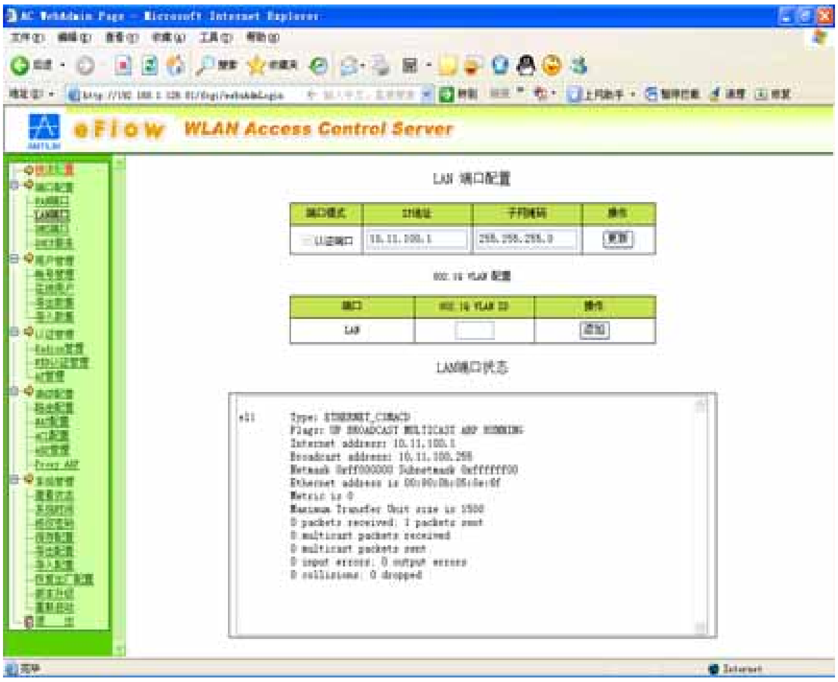
PPPoE 帐号设置：如果使用 ADSL/xDSL 时，可以选择 PPPoE 作为 WAN 端口的接入模式，

在此设置中写入从 ISP 那里获得的 PPPoE 的帐号和密码。

WAN 端口状态：显示此端口的状态信息，包括 IP 地址、收发包情况等。

设置完成后点击 “ 更新 ” 按钮使设置生效

3.3.2. LAN 端口（E1 口）配置



端口模式：LAN 强制为需要认证模式，此端口下的用户为受控制的用户。如果此端口下用户不需要认证，可以在 WEB 认证配置中，把用户设置为直通模式；

IP 地址：配置端口的 IP 地址，如果 WACS 作为网关使用，此端口下的用户网关地址就是 LAN 端口的 IP 地址；

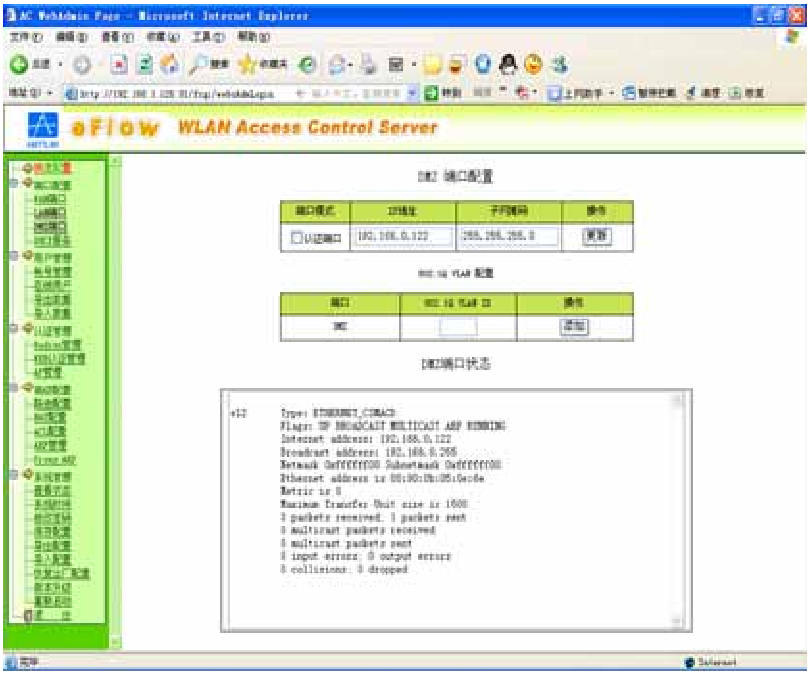
子网掩码：配置端口的子网掩码；

LAN 端口状态：显示此端口的状态信息，包括 IP 地址、收发包情况等。

修改后，请点击 “ 更新 ” 按钮，是更新生效。

802.1Q VALN 设置：如果网络中使用了 802.1Q VALN 的设置，请将交换机的上行端口连接到 LAN 端口上，并输入所使用的 VLAN ID 号，点击“ 添加 ”按钮，把所输入的 VLAN ID 加到端口的 802.1Q VALN 设置中。如果不需要把交换机的 VLAN TAG 上传，不需要对此进行配置（建议不上传 VLAN TAG）。

3.3.3. DMZ 端口（E2 口）配置



端口模式：选择使用此端口的用户是否需要认证，DMZ 端口默认为非认证模式，此端口下可以放置一些公用的服务器或者其他的共享服务器；

IP 地址：配置端口的 IP 地址，如果 WACS 作为网关使用，此端口下的用户网关地址就是 DMZ 端口的 IP 地址；

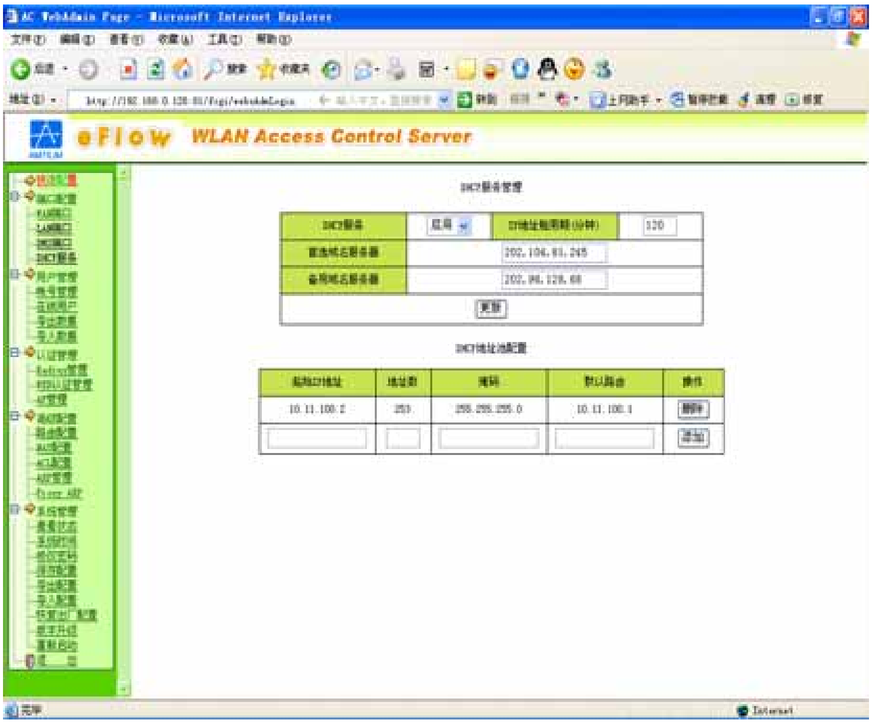
子网掩码：配置端口的子网掩码；

DMZ 端口状态：显示此端口的状态信息，包括 IP 地址、收发包情况等。

修改后，请点击“ 更新 ”按钮，是更新生效。

802.1Q VALN 设置：如果网络中使用了 802.1Q VALN 的设置，请将交换机的上行端口连接到 DMZ 端口上，并输入所使用的 VLAN ID 号，点击“ 添加 ”按钮，把所输入的 VLAN ID 加到端口的 802.1Q VALN 设置中。如果不需要把交换机的 VLAN TAG 上传，不需要对此进行配置（建议不上传 VLAN TAG）。

3.3.4. DHCP 服务管理



DHCP 服务管理：WACS 上内置了 DHCP Server。在此菜单中对其进行配置管理。

DHCP 服务：如果需要使用 WACS 内置的 DHCP Server 时，选择启用 DHCP 服务；否则，选择禁用 DHCP Server。（系统默认 DHCP Server 为启用）

IP 地址租用期：IP 地址租用期是指 DHCP 获取地址的有效时间，DHCP 客户端会根据这个时间进行地址的重新续租。如果网络中的用户变动比较频繁，可以适当调小 IP 地址的租用期；如果网络中用户比较固定时，可以适当调大 IP 地址的租用期。

首选域名服务器：DHCP 用户分配的域名服务器 IP 地址。

备用域名服务器：DHCP 用户分配的备用域名服务器 IP 地址。

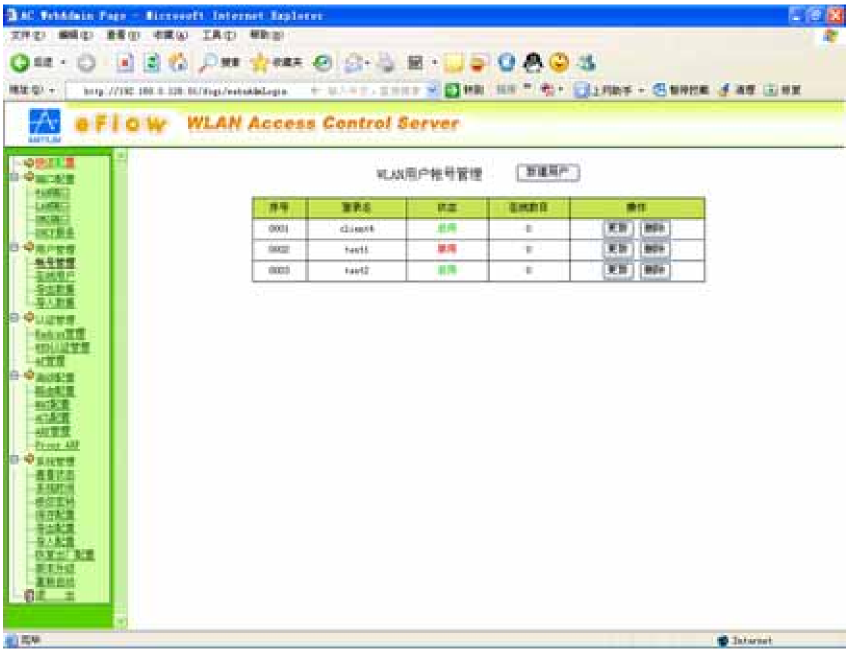
DHCP 地址池配置：DHCP 用户分配的 IP 地址段，可以分配多个地址段，每个地址池最大可分配的地址数限制在 2550 个，超过此数，为非法操作。（注意：只有在需要认证的端口上才可以使用 DHCP 获得地址，所以 DMZ 端口默认是不可以分配地址的）

3.4. 用户管理

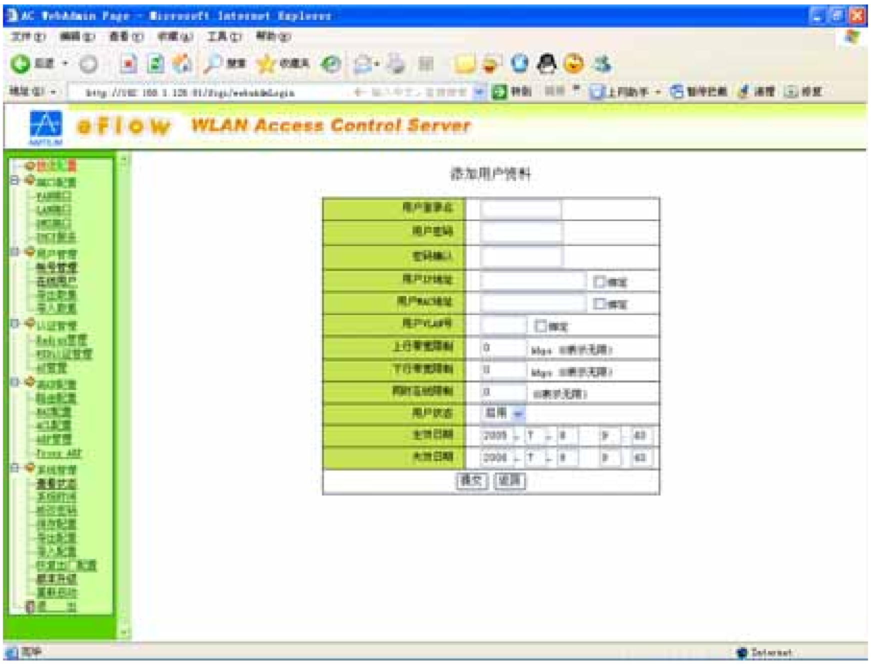
用户管理完成对用户帐号的管理，实现用户数据的导入导出。

3.4.1. 帐号管理

管理 WLAN 用户帐号，包括新建用户、更新帐号、删除帐号。



新建用户：如果需要添加一个新的用户帐号，点击“ **新建用户** ”按钮，新建一个用户帐号，需要在**添加用户资料**界面中输入下面的用户信息：



用户登录名：用户认证使用的用户登录名，也就是用户的帐号；

用户密码：用户认证时使用的密码，密码需要输入两次确认，以避免输入错误；

用户的 IP 地址：如果网络中的部分用户使用静态 IP 地址，同时要求控制这些用户只能时使用该 IP 地址时，可以填入用户帐号对应的 IP 地址，选择与用户的帐号绑定，这样这个帐号就只能使用所绑定的 IP 地址来访问 Internet；(认证点在 WACS 时，此项才起作用，如果认证点在 AP，此绑定不起作用）

注意：IP 地址格式为：xxx.xxx.xxx.xxx（例如 192.168.1.126）

用户 MAC 地址：如果某些帐号只允许在某些电脑上使用时，输入该电脑网路适配器的 MAC 地址，并选择与帐号绑定。这个用户帐号就只能在这个网络适配器上使用；

注意：MAC 地址格式为：xxxxxxxxxxxx（字母请使用小写，例如 780f17391e70）

用户的 VLAN 号：如果网络中使用 802.1QVLAN 设置时，同时希望某些帐号只能在某个固定的 VLAN 中使用时，可以把用户使用那个 VLAN ID 和用户的帐号绑定起来；（认证点在 WACS 时，此项才起作用）

上行带宽限制：如果网络中有多台电脑在同时使用时，为了更好的利用资源，可能需要对用户的上行带宽进行控制，这里的带宽限制是以 **32Kbit** 为步长进行控制的（认证点在 WACS 时，此项才起作用）；(注意：当为 0 时，用户带宽不受限制)

下行带宽限制：如果网络中有多台电脑在同时使用时，为了更好的利用资源，可能需要对用户的下带宽进行控制，这里的带宽限制是以 **32Kbit** 为步长进行控制的（认证点在 WACS 时，此项才起作用）；(注意：当为 0 时，用户带宽不受限制)

同时在线数限制：如果需要为同一类用户使用统一帐号时，可能需要控制同一帐号的同时在线人数，填入规定好的同时在线人数时，如果此帐号在线人数达到你规定的数目时，再使用这一帐号登录的用户就将不会通过认证（认证点在 WACS 时，此项才起作用）；(注意：当为 0 时，用户同时在线数不受限制)

用户状态：如果需要停用某个帐号但又不想删除该帐号时，或者需要拥有一些灵活使用

的帐号（这些帐号可以在使用时激活，是用完以后禁止），可以通过控制用户帐号的启用和禁止来达到灵活使用目的；

生效日期：指定帐号开始生效的日期，精度可以指定到分钟；

注意，日期输入的格式为（YYYY-MM-DD HH:MI，YYYY 是年份，MM 是月份，DD 为日期，HH 为小时，MI 为分钟）

失效日期：指定帐号失效的日期，精度可以指定到分钟。输入格式同生效日期。

输入完信息后，按提交，用户资料将被保存在内存中，如果需要永久保存用户帐号，需要保存配置。

更新用户资料：如果需要更新某用户的资料，在用户列表中该用户的后面，点击“ 更新 ”按钮，进入修改用户资料的界面，此界面与添加用户资料界面相同，请参考新建用户

删除用户资料：如果要删除某些用户的资料，点击“ 删除 ”按钮，将出现询问界面，一旦确认，就可以删除那些不再使用的用户资料。注意：请确认这些用户资料不再需要，一旦确认，保存配置后，该用户帐号资料将不可恢复，使用该帐号的用户均无法登录。

3.4.2. 在线用户

如果认证点在 WACS，可以查看在线的认证用户。内容包括：正在使用的帐号、该帐号使用的 IP 地址、该帐号使用的 MAC 地址、该帐号的状态和登录时间。同时，也可以对认为不合法的用户实行强制下线。

3.4.3. 导出数据

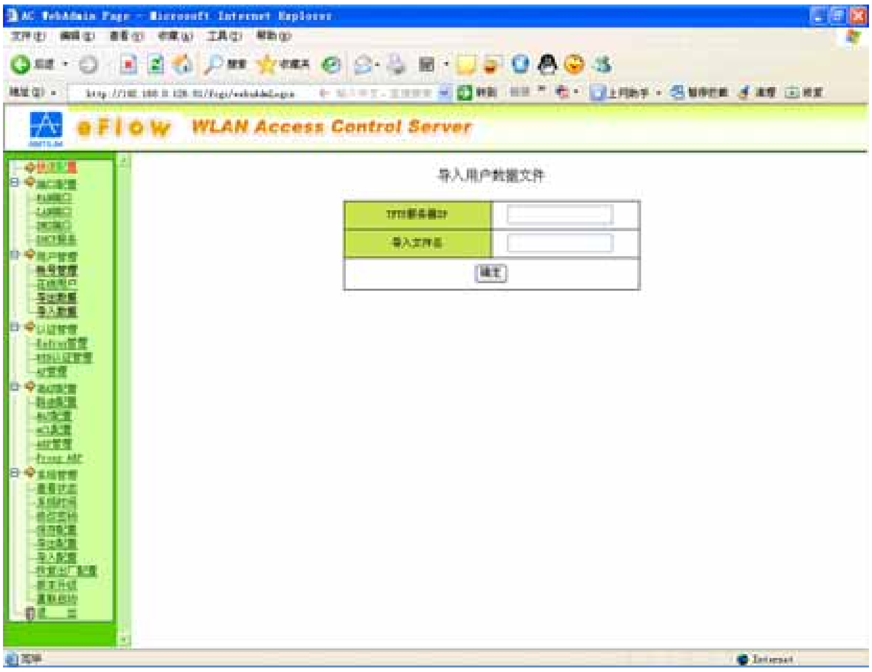
如果需要把用户数据导出到其他存储设备保存，以防用户资料丢失，可以使用导出用户数据。导出数据使用的是 TFTP 工具，需要在接收数据的机器上启动 TFTP 服务器。

TFTP 服务器 IP：填写 TFTP 服务器的 IP 地址。

导出文件名：填写在 TFTP 服务器上保存用户数据的文件名。（请注意 TFTP 服务器的路径，确保用户数据文件正确的保存，导出的文件为文本格式，可以直接用文本编辑器查看）

3.4.4. 导入数据

如果需要恢复 WACS 的用户数据，请使用导入数据的功能来恢复以前备份下来的用户数据。



TFTP 服务器 IP：填写 TFTP 服务器 的 IP 地址。

导出文件名：填写将从 TFTP 服务器上获取的用户数据的文件名。（请注意 TFTP 服务器的路径，确保用户数据文件在相同目录下）

3.5. 认证管理

认证管理完成对认证元素的设置，包括 Radius、WEB 认证、AP 的管理等。

3.5.1. Radius 管理

Radius 管理包括对 Radius 服务和 Radius Client 的管理。Radius 服务是 WACS 内带的模块，可以选择启用或者禁用。本地 Radius 服务使用的端口为 1812 和 1813。

Radius Client 是在有外接 Radius 服务器的情况下，使用 WACS 作为认证点，需要配置 WACS 作为 Radius Client，转发 Radius 请求到指定的外接 Radius 服务器。

本地 Radius 服务： WACS 内置了 Radius 服务器，根据需要决定是否使用本地 Radius 服务。如果使用本地 Radius 服务时，可以不需要外置的 Radius 服务器，直接处理下面的 AP 发过来的 Radius 请求。本地 Radius Server 只提供认证和授权功能，并不涉及计费问题，所以本地 Raidus 服务不提供详细的上网记录清单。

Radius Client 部分的设置内容如下：

项目：WACS 提供了首选认证服务器、首选计费服务器、备用认证服务器、备用计费服务器、复制计费服务器。其中首选和备用服务器构成主、备服务器，复制计费服务器仅可以提供用户的上网纪录；

服务器地址：Radius 服务器的 IP 地址。

Radius KEY：用于 Radius 协议互相协商的加密密钥

UDP 端口：Radius 协议端口，在较旧的 RFC 中规定为：认证端口：1645、计费端口：1646，新 RFC 标准为：认证端口：1812、计费端口：1813。可以在这里填写和 Radius Server 相应的端口号。

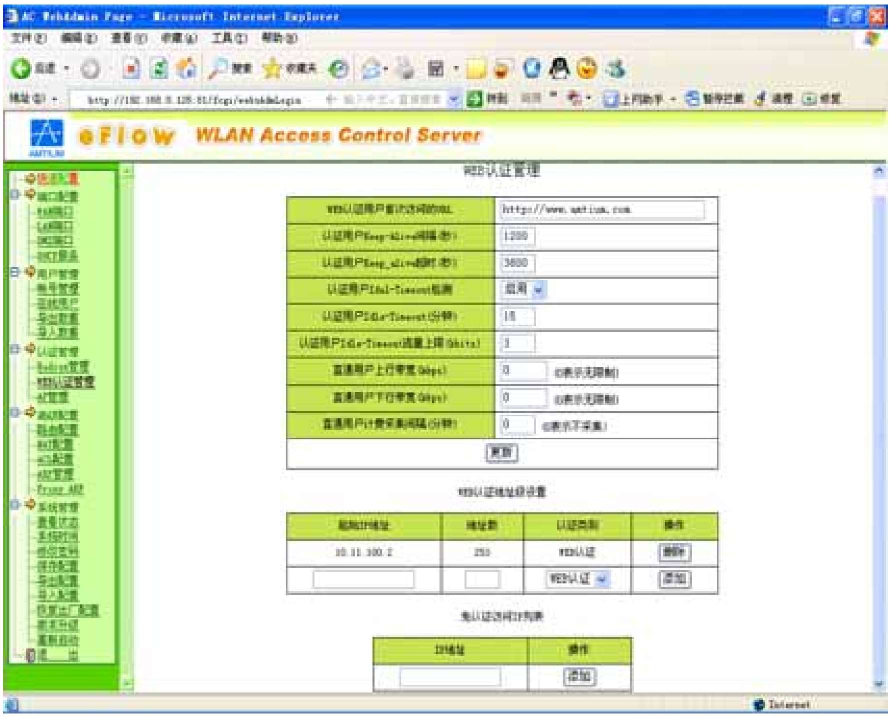
超时：发出 Radius 请求后，在设定的时间内没有收到 Radius Server 的回应，就认为认证超时。这里是设置超时时间，单位 S。

重发：当认证出现超时时，重发的认证请求次数。

启用：是否启用该项 Radius 配置。

3.5.2. WEB 认证管理

如果使用 WACS 作为认证点，在此对认证的属性进行设置，主要内容包括：认证后用户首次访问的 URL、认证保持连接的属性、控制用户进行认证的地址、不需要认证可以访问的地址等。



WEB 认证用户首次访问的 URL：用户认证后，可以强制用户访问的第一个 WEB 页面，方便公司或者 ISP 发布一些通知或者其他的公告信息。输入此页面的 URL，用户认证后，将会在浏览器中直接看到对应的 WEB 内容。

认证用户 Keep_Alive 间隔：设置对在线状态判断的时间间隔（单位 秒）。每隔一定的时间，与用户的连接小窗口进行一次对话，确认用户是正常在线使用。

认证用户 Keep_Alive 超时：这个选项是和上面的配合使用的，配置了检查的间隔后，需要设置多长时间才把用户从在线表中删除，并释放资源。如果在设定的时间内，WACS 和用户的连接小窗口没有进行过连接对话，将把用户从在线表中删除，如果用户需要上网，需要重新进行认证。注意：这里的时间应设为 Keep_Alive 间隔的整数倍。

认证用户 Idle_Timeout 检测：很多浏览器设置了拦截弹出小窗口的功能，在使用 WEB 认证时，就会出现用户无法和 WACS 保持连接对话的情况，造成用户在 Keep_Alive 超时过后，就需要重新认证。为了避免这种情况，WACS 提供了用户流量空闲检查的功能。当某个用户在规定时间内的流量少于上限流量就认为该用户处于闲置状态，应该回收分配给他的资源。根据具体的网络使用情况确定是否使用此功能。（如果出现这种情况，应该把 Keep_Alive 的检查和超时时间设置为很长，例如检查间隔为 3600 秒，超时为 10800 秒）

认证用户 Idle_Timeout：进行闲置在线的检查的时间间隔，单位 秒。

认证用户 Idle_Timeout 流量上限：在规定时间间隔内，用户必须达到这个规定的流量（单位 Kbits），否则认为用户闲置，断开其连接，如果对在线的检查不需要很严格，可以把 Idle_Timeout 设置长一些，同时把流量上限设置低一些。

直通用户上行带宽：如果网络中存在一部分不需要认证的 IP 地址段时（如何配置请看 WEB 认证地址段)，但是希望对他们的上行带宽也进行限制，在这里进行设置。(步长 :32Kbits，单位：Kbits，0 表示不限带宽)

直通用户下行带宽：如果网络中存在一部分不需要认证的 IP 地址段时（如何配置请看 WEB 认证地址段)，但是希望对使用这段地址的用户的上行带宽也进行限制，在这里进行配置。(步长：32Kbits，单位：Kbits，0 表示不限带宽))

直通用户计费采集间隔：如果网络中存在一部分不需要认证的 IP 地址段时（如何配置请看 WEB 认证地址段)，同时使用了外置的 Radius Server 来获取用户上网的详细清单时，可以设置计费采集间隔，可以提供该用户上网的时间，使用的 IP，使用时长，出流量，入流量、入字节、出字节等等用户上网信息。

WEB 认证地址段：可以对 LAN 端口的地址进行规划，划分需要认证或者不认证（直通）的用户。如果地址不在认证地址段中，用户将无法访问 WACS 外面的网络资源，网络地址需要仔细规划，各段之间不要重复，也不要把 WACS 的端口地址包含在认证地址段中。

起始 IP 地址：需要控制的地址段的起始地址；

地址数：起始地址后面连续的地址数；

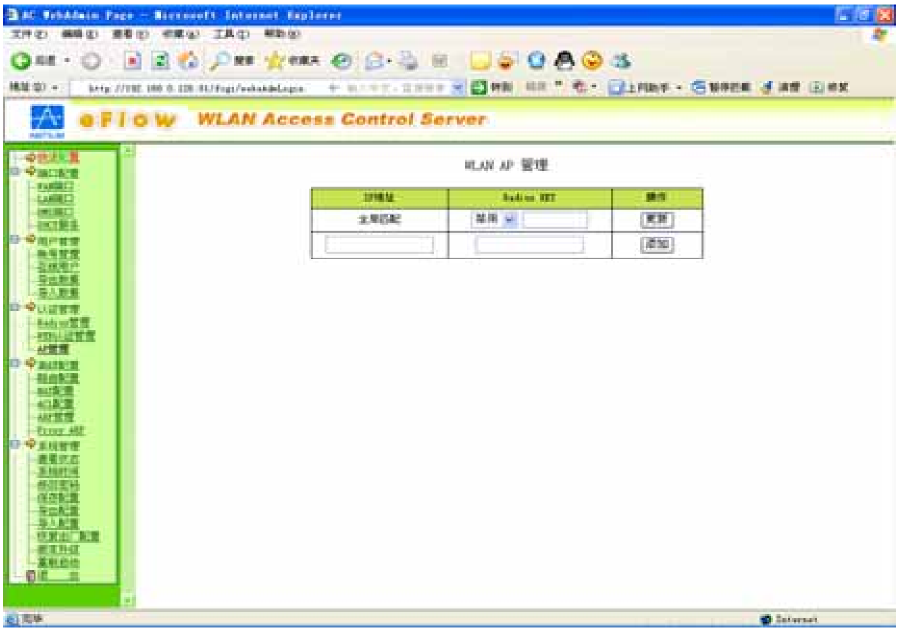
认证方式：认证方式有直通和 WEB 认证两种方式，如果是直通，用户不需要认证，即可以直接上网，如果是 WEB 认证，用户需要认证才能上网；

免认证访问 IP 列表：如果网络中使用了一些公用的服务器时（在 WACS 的 WAN 端口外或者 DMZ 端口中），希望在用户不认证的情况下也可以访问，可以配置这些服务器的 IP 地址，最多可以添加 8 个免认证访问的 IP 地址。

IP 地址：免认证的服务器的 IP 地址

3.5.3. AP 管理

如果认证点在 AP，启用 WACS 的 Radius 服务，需要对 AP 进行管理，主要是配置接受哪些 AP 的认证包，以及使用的 Radius 认证密钥。



IP 地址：如果 AP 使用的密钥每一个都不相同的话，需要把每个 AP 的地址和 Radius KEY 添加进去。如果所有 AP 使用同一个密钥，可以使用全局匹配，把所有 AP 使用的 Radius KEY 都配置为全局密钥。

禁用/启用：禁用或者启用全局匹配 Radius KEY。

Radius KEY：每个 AP 使用的 Radius KEY。此 Radius KEY 用于 AP 和 WACS 内置的 Radius 服务器进行通信使用。

3.6. 高级配置

高级配置是针对 WACS 的一些网络方面的管理和安全功能进行配置，包括静态路由、NAT、ACL 等。

3.6.1. 路由配置

配置和查看 WACS 的静态路由信息。

IP 静态路由配置：如果网络环境比较复杂时，特别是网络中含有三层设备时，需要对 WACS 进行静态的 IP 路由设置。

目的地址：要访问的目的的 IP 地址。

目的地址掩码：要访问的目的地址的掩码。

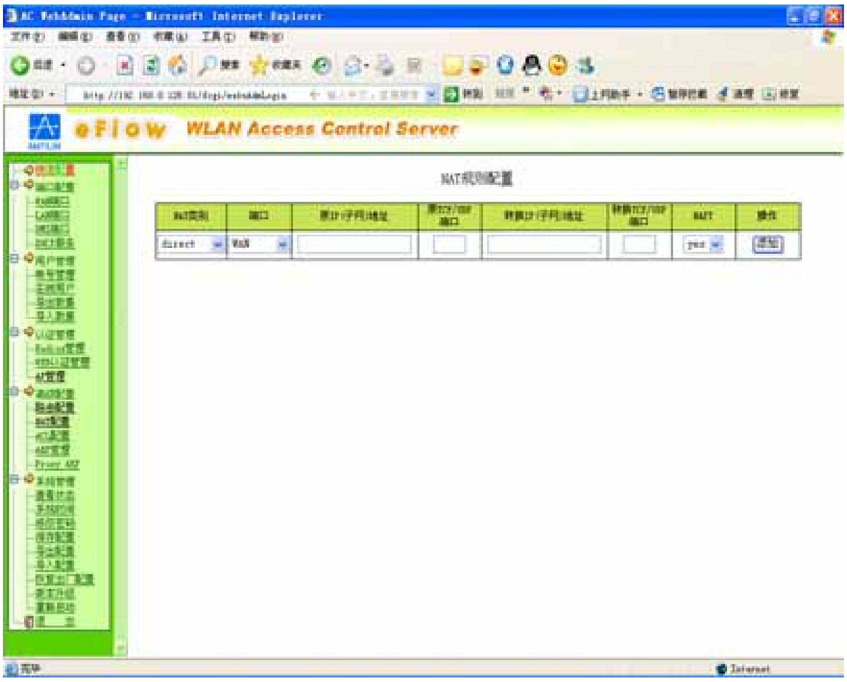
下一跳地址：下一跳的路由器的 IP 地址。

如果 WAN 端口使用静态 IP 时，配置的 WAN 端口的网关，就是 WACS 的默认路由。

当前系统 IP 路由表信息：显示当前 WACS 的路由表，可以方便查找和配置。

3.6.2. NAT 配置

如果 ISP 只提供给一个或者几个 IP 地址时，需要使用网络地址转换功能（NAT），当在配置 WAN 端口时使用了自动 NAT 的时候,所有的下行地址都会被自动转换到 WAN 端口的 IP 地址上。



NAT 类别：WACS 提供两种 NAT 转换模式：direct 和 redirect。direct 是正向映射地址，对源地址进行映像，改变数据包的源地址，对数据的目的地址不做任何改变；redirect 是反向映射，对目的地址进行改变，重新定向数据的目的地址，对数据的源地址不做任何改变。

注：使用 redirect 规则时，复位指向的地址只能是一个，因此掩码都应该是 32

端口：在 WACS 的哪个端口上使用 NAT 功能，分别为 WAN、LAN、DMZ、WANppp0。

源 IP 子网：需要进行地址转换的私网子网，格式为 IP/Prefix。其中，IP 位网络地址，Prefix 为地址中网络部分所占位数。（例如 10.1.1.0/24）

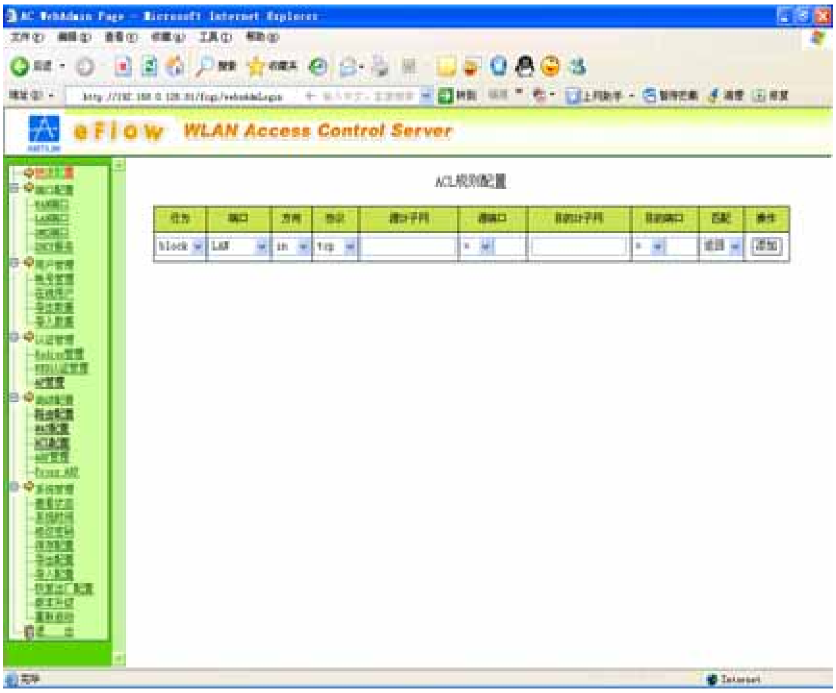
原 TCP/UDP 端口：用于 redirect 规则，指定目的地址的端口，可选

转换 IP 子网：转换的目的 IP 地址。格式为 IP/Prefix。其中，IP 位网络地址，Prefix 为地址中网络部分所占位数。（例如 10.1.1.0/24）

NAPT：是否用端口动态映射，用于 direct 规则，可选

3.6.3. ACL 配置

现在网络越来越重视网络安全问题，WACS 提供了 IP 地址和端口的过滤功能



行为：block：阻塞　pass：通过。

端口：ACL 规则适用于哪个端口，包括 WAN、LAN、DMZ、WANppp0。

方向：in：对流入包进行控制，out：对流出包进行 ACL 控制。

协议：针对哪种协议使用 ACL 规则。可选 TCP、UDP 和 ICMP 协议。

源 IP 子网：ACL 控制针对源 IP 子网，格式为 IP/Prefix。其中，IP 位网络地址，Prefix 为地址中网络部分所占位数。如果要对某一端口所有地址进行 ACL 控制时，请使用 0.0.0.0/0 的格式。

源端口：（可选）配置 ACL 控制针对源端口，

端口匹配方式（比较符）：'=' 等于、'!='不等于、'>'大于、 '>=' 大于或等于、 '<'小于 、'<='小于或等于；

端口号：添入端口号的数值。

目的 IP 子网：ACL 控制针对目的 IP 子网，格式为 IP/Prefix。其中，IP 位网络地址，Prefix 为地址中网络部分所占位数。如果要对某一端口所有地址进行 ACL 控制时，请使用 0.0.0.0/0 的格式。

目的端口：(可选）配置 ACL 控制针对目的端口，

端口匹配方式（比较符）：'=' 等于、'!='不等于、'>'大于、 '>=' 大于或等于、 '<'小于 、'<='小于或等于；

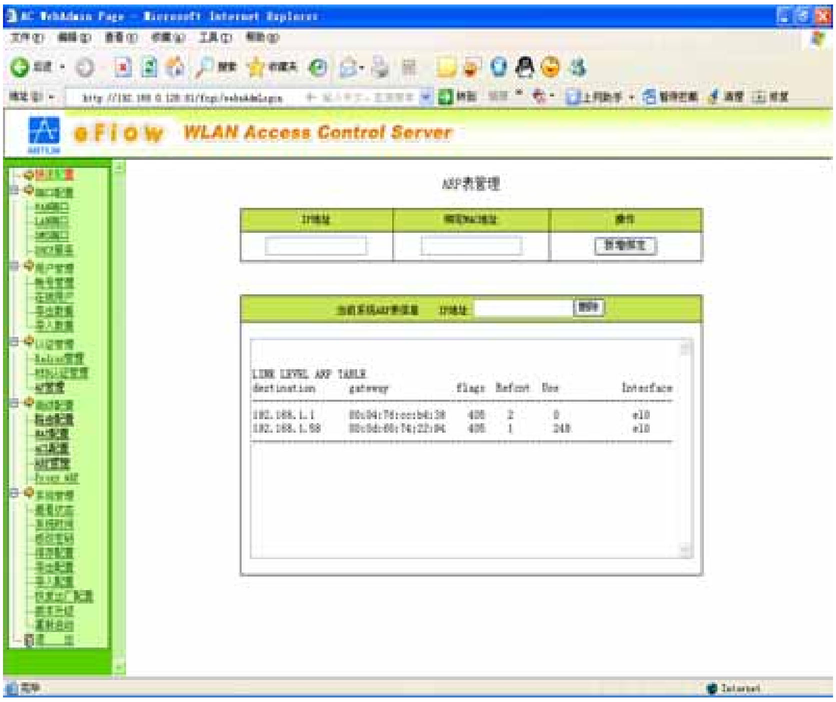
端口号：添入端口号的数值。

匹配：返回：找到合适的规则后就直接返回，不再往下进行规则匹配。

继续：找到规则后不直接返回，继续往下进行规则匹配，直到匹配完所有规则。

3.6.4. ARP 管理

由于 WLAN 的开放性，所以比较容易出现 IP 地址冲突，出现 IP 冲突时，可能导致一些用户不能正常访问网络，解决的办法之一，就是对 WACS 上的 ARP 表进行管理。可以把某些 IP 和 MAC 地址绑定起来。



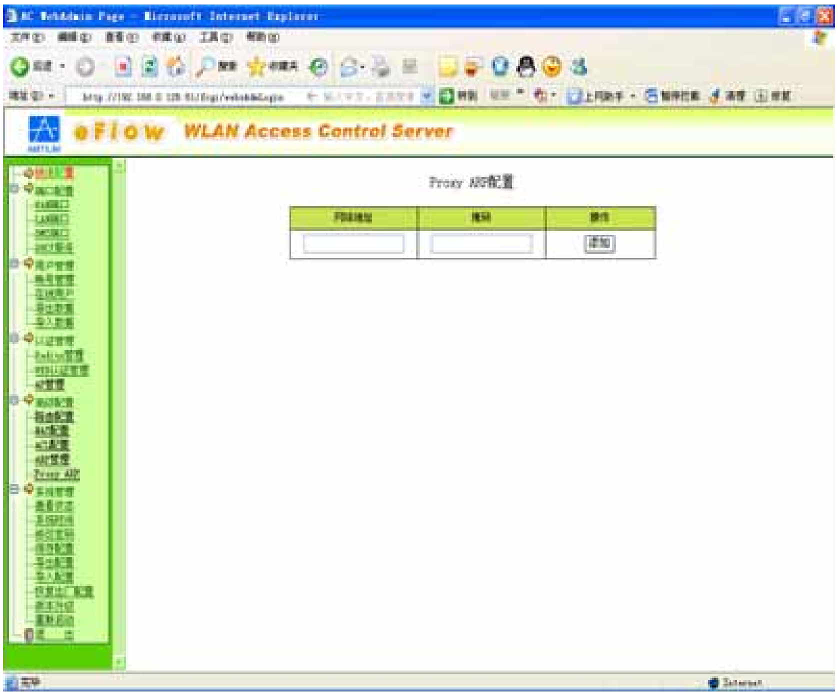
IP 地址：输入对应固定 MAC 地址的 IP。

绑定 MAC 地址：输入固定使用某 IP 地址的网络适配卡 MAC 地址；

当前系统 ARP 表信息 ：显示当前系统 ARP 表信息，同时，可以删除某些非法的 ARP 信息，只需要输入 IP 地址，然后点击 " 删除 " 按钮即可。

3.6.5. Proxy ARP

如果 ISP 给提供了一段连续的 IP 地址时，而只使用一个作为 WAN 端口的地址，其他地址就没有使用而浪费。这时，可以使用该项配置，代理其他同段地址的 ARP 响应。同时，在连接 LAN 或者在 DMZ 端口的交换机上配置了 VLAN 或者端口隔离，为了使用户之间可以互访，也可以通过代理用户地址端的 ARP 响应，使用户可以互访。



网络地址：输入被代理子网的网络地址。

掩码：输入被代理子网的网络掩码。网络地址和掩码必须严格按照规范输入，否则代理规则将不会有作用。

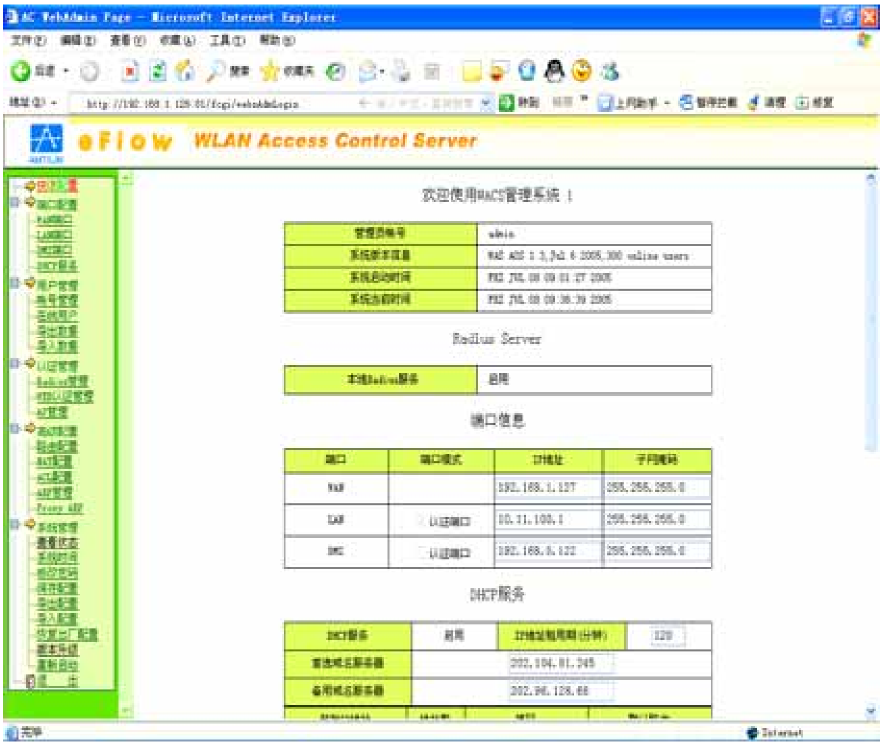
3.7.系统管理

系统管理是对系统时间、管理密码、设备配置、版本升级等内容进行设置管理。

3.7.1. 查看状态

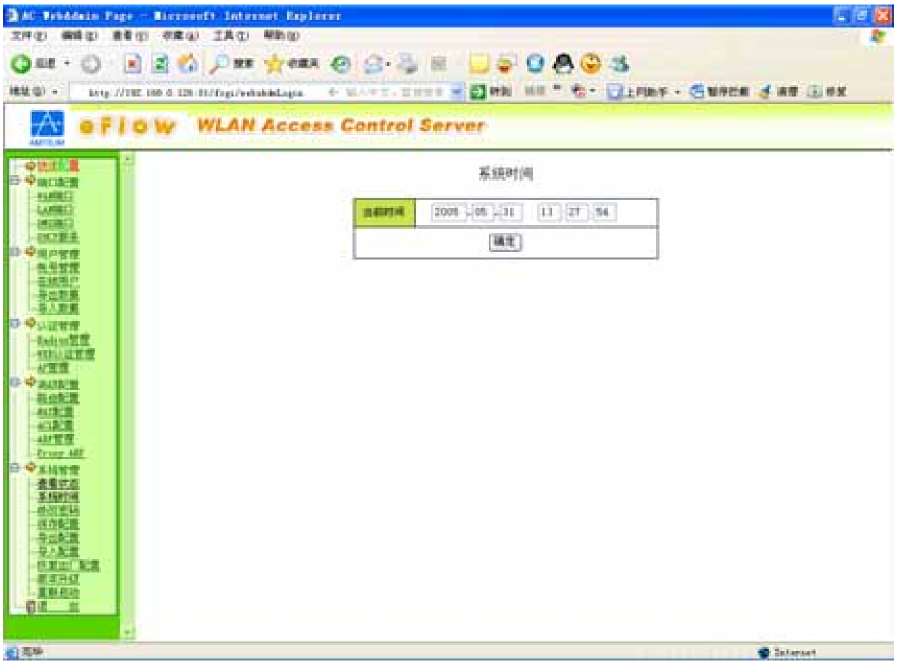
进入管理界面的第一个页面就是查看状态。

显示系统的当前版本、时间、主要配置等内容。如下图：



3.7.2. 系统时间

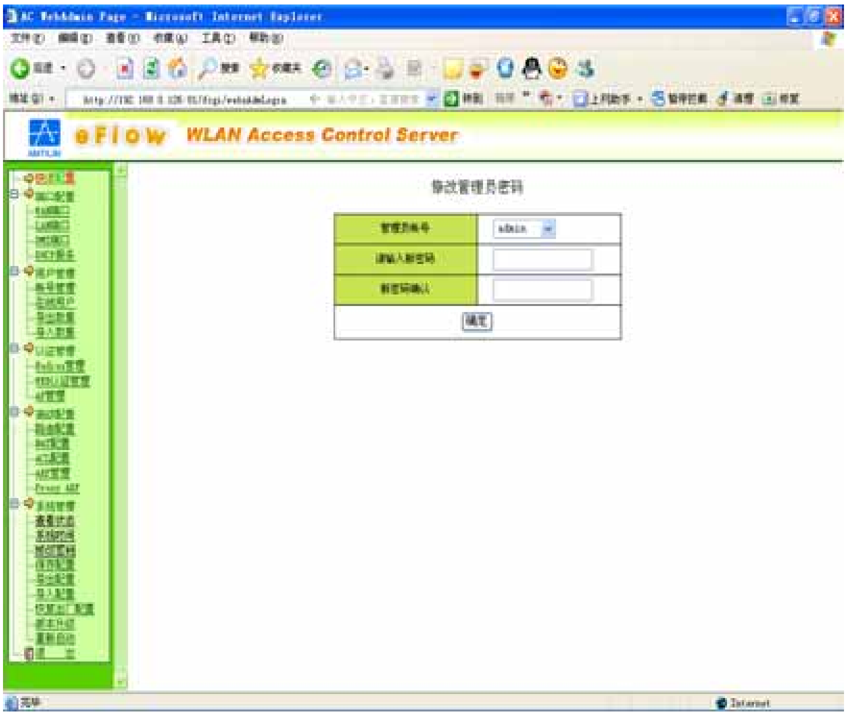
可以修改 WACS 的系统时间。



输入当前准确的年、月、日、时、分、秒，点确定，即可修改当前的系统时间。

3.7.3. 修改密码

只有 admin 用户才能修改密码，manager 用户不能修改密码。选择要修改密码的用户，输入密码和密码确认，点击确认修改选择用户的密码。



3.7.4. 保存配置

点击 “ 保存设置 ”，就会出现 “ 保存操作成功 ” 的提示，表示已经把当前的修改全部保存起来。在更改任何属性后，都需要保存起来。否则，机器重新启动后，修改的配置将遗失。

3.7.5. 导出配置

可以把在 WACS 中保存的设备配置文件导出到另外的机器保存，以备以后配置丢失再导入 WACS 中。导出配置是通过 TFTP 工具进行，在接收配置的机器上必须开启 TFTP 服务器。

TFTP 服务器 IP：填写 TFTP 服务器的 IP 地址。

导出文件名：填写在 TFTP 服务器上保存配置的文件名。（请注意 TFTP 服务器的路径，确保配置文件正确的保存，导出的文件为文本格式，可以直接用文本编辑器查看）

3.7.6. 导入配置

可以把保存的配置，通过 TFTP 工具，导入到 WACS 中。

导入成功后，需要重新启动设备，配置才能生效。在重启设备前，切记不要保存配置，否则导入的配置文件将被当前的运行配置覆盖。

TFTP 服务器 IP：填写 TFTP 服务器 的 IP 地址。

导出文件名：填写将从 TFTP 服务器上获取的配置文件的文件名。（请注意 TFTP 服务器的路径，确保配置文件在相同目录下）

3.7.7. 恢复出厂配置

可以恢复 WACS 到出厂的配置状态，恢复后，需要重新启动设备。重新启动前，不要保存配置，否则出厂配置将被当前配置覆盖。

点击确定，将重写配置文件到出厂配置状态。

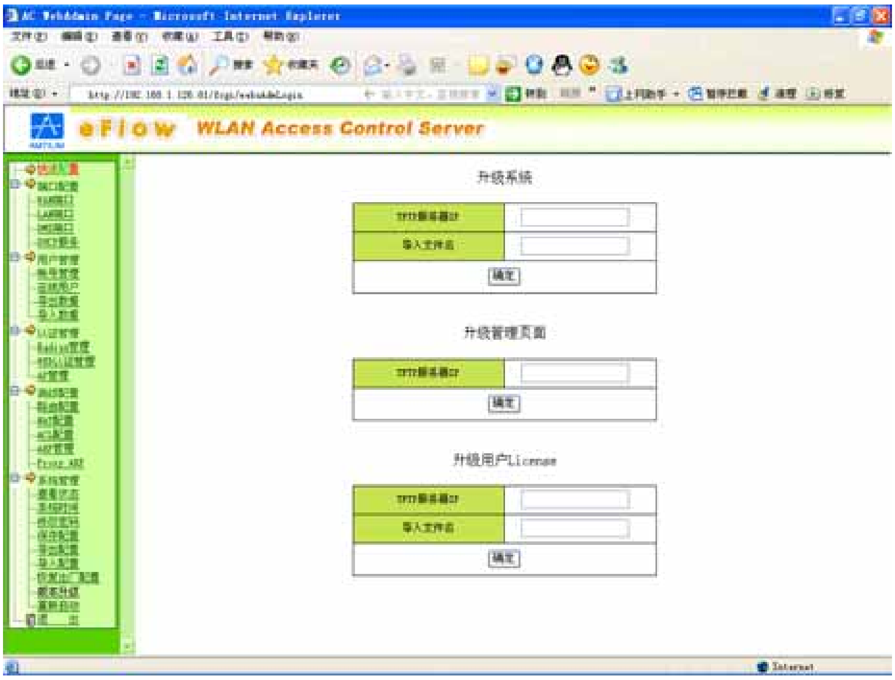
3.7.8. 版本升级

如果需要更新到最新的版本，可以用 TFTP 工具把 WACS 设备升级到指定的新版本。

如果需要更新设备的用户 License 信息，同样也是通过 TFTP 工具进行升级。

升级版本有三部分内容：升级系统、升级管理页面、升级用户 License。

升级系统是对 WACS 的操作系统进行升级。升级管理页面是把管理界面，也就是现在看到的页面更新到最新的内容。升级用户 License 是更新设备的 License 信息。



升级系统运行版本的正确步骤应该是：先升级系统，重新启动 WACS，让新系统运行，然后再升级管理页面。

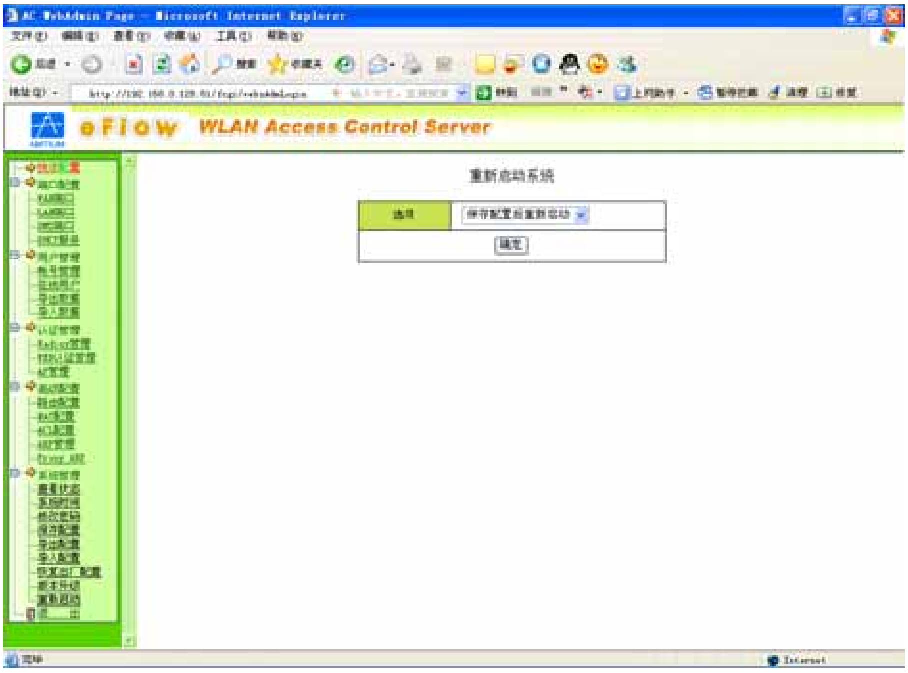
如果是升级用户 License，可以直接进行操作，不需要进行系统和管理页面的升级。

TFTP 服务器 IP：填写 TFTP 服务器的 IP 地址。

导出文件名：新版本系统的文件名。

3.7.9. 重新启动

修改了系统的属性以后，需要重新启动 WACS，这里的启动包括了“保存设置后重新启动”和“不保存设置重新启动”两种方式。确认修改正确时，使用“保存设置后重新启动”；如果修改的配置出现问题，或者想使用未修改的前的配置，使用“不保存配置重新启动”。



4. 使用范例

为方便理解，下面针对几种比较常用的情况，进行简单的描述。

4.1. AP 作为认证点，WACS 启用控制

环境描述：认证点在 AP，WACS 需要对网络进行隔离，把用户和服务器的网络分开，

防止非认证的用户可以直接访问服务器资源。

连接方法：把服务器和其他的公用服务资源连接在 WACS 的 DMZ 端口（E2 口），AP 组成的网络连接在 WACS 的 LAN 端口（E1 口），WACS 的 E0 口连接网络出口，或者上层网络的端口上。

配置要点：

一、配置 WAN 端口（端口配置->WAN 端口配置），把此端口的地址设为分配的出口地址（或者上层网络分与的地址），如果需要做地址转换，选择自动 NAT 项

二、配置 LAN 端口(端口配置->LAN 端口配置),把此端口设置为 AP 网络段的地址(一般是作为此网段的网关）

三、配置 DMZ 端口（端口配置->DMZ 端口配置），把此端口设置为服务器网络的地址（一般是作为此网段的网关）

四、配置本地的 Radius 服务（认证管理->Radius 管理），启用本地 Radius 服务

五、配置缺省路由（高级配置->路由配置），把 WACS 的缺省网关指向上层的网关

六、添加 AP（认证管理-> AP 管理），配置好 AP 和 WACS 内置 Radius 的共享密钥

七、配置需要认证的地址段（认证管理->WEB 认证管理），由于认证点在 AP，所有用户地址段都配置成直通类型

八、保存配置（系统管理->保存配置）

九、添加用户帐号（用户管理->帐号管理）

配置完成后，用户使用 802.1x 客户端认证以后即可上网。

方案特点：

一、使用 802.1x 认证，增加了网络的安全性

二、WACS 把用户认证的网络和服务器网络隔离，可以保证非法用户不能访问服务器资源

三、WACS 在网络的出口，可以利用 WACS 本身的 ACL 对网络安全进行基本的保护

四、可以直接使用 WACS 的 NAT 功能，让多人同时共享上网

五、启用 WACS 的本地 Radius 和用户管理功能，简化了网络管理的负担

4.2. AP 作为认证点，WACS 只启用认证服务

环境描述：认证点在 AP，WACS 只需要提供认证和用户管理。

连接方法：直接把 WACS 的 WAN 端口（E0 口）接入到网络中，其他端口可以不连接

配置要点：

一、配置 WAN 端口（端口配置->WAN 端口），把此端口的地址设为分配的出口地址（或者上层网络分与的地址），不需要做 NAT 转换

二、配置本地的 Radius 服务（认证管理->Radius 管理），启用本地 Radius 服务

三、添加 AP（认证管理-> AP 管理），配置好 AP 和 WACS 内置 Radius 的共享密钥

四、如果 AP 所在的网络和 WACS 不在同一网段，还需要配置 WACS 的缺省路由（高级配置->路由配置）

五、保存配置（系统管理->保存配置）

六、添加用户帐号（用户管理->帐号管理）

配置完成后，用户使用 802.1x 客户端认证以后即可上网。

方案特点：

一、使用 802.1x 认证，增加了网络的安全性

二、启用 WACS 的本地 Radius 和用户管理功能，简化了网络管理的负担

三、WACS 只作为认证服务器使用，对原有的网络结构几乎不用变动，同时，增强了网络的安全性

四、对于出口地址比较多，使用了 VPN 服务器、防火墙的网络，采用这种方案对网络结构影响最小，能够做到和原来网络无缝连接

4.3. WACS 作为认证点，启动 WEB 认证

环境描述：认证点在 WACS，AP 只是透明的网桥，采用 WEB 认证。

连接方法：把服务器和其他的公用服务资源连接在 WACS 的 DMZ 端口（E2 口），AP 组成的网络连接在 WACS 的 LAN 端口（E1 口），WACS 的 WAN 端口（E0 口）连接网络出口，或者上层网络的端口上。

配置要点：

一、配置 WAN 端口（端口配置->WAN 端口），把此端口的地址设为分配的出口地址（或者上层网络分与的地址），如果需要做地址转换，选择自动 NAT 项

二、配置 LAN 端口（端口配置-> LAN 端口），把此端口设置为 AP 网络段的地址（一般是作为此网段的网关）

三、配置 DMZ 端口（端口配置->DMZ 端口），把此端口设置为服务器网络的地址（一般是作为此网段的网关）

四、如果使用外置的 Radius Server，在认证管理->Radius Client 中进行配置，否则，不用进行 Radius 配置

五、配置缺省路由（高级配置->路由配置），把 WACS 的缺省网关指向上层的网关

六、配置需要认证的用户地址段（认证管理->WEB 认证管理），用户分为 WEB 认证和直通用户两种，根据需要进行配置

七、如果需要启用 DHCP 服务，在端口配置->DHCP 服务管理中配置正确的地址池，如果不需要，则不用地址池，直接禁用 DHCP 服务。

八、保存配置（系统管理->保存配置）

九、添加用户帐号

配置完成后，用户可以通过浏览器认证上网。

方案特点：

一、AP 不作为认证点，只需要当做透明网桥

二、采用 WEB 认证，不需要特别安装或配置客户端软件

三、WACS 把用户认证的网络和服务器网络隔离，可以保证非法用户不能访问服务器资源，基本保证网络资源的安全

四、WACS 在网络的出口，可以利用 WACS 本身的 ACL 对网络安全进行基本的保护

五、可以直接使用 WACS 的 NAT 功能，让多人同时共享上网

六、启用 WACS 的本地 Radius 和用户管理功能，简化了网络管理的负担

5. 出厂配置主要内容

- 端口配置

WAN 端口 192.168.0.126 / 255.255.255.0　静态 IP　自动 NAT 不启用

LAN 端口　10. 11.100.1 / 255.255.255.0　认证端口

DMZ 端口　192.168.1.122 / 255.255.255.0　非认证端口

- DHCP 服务

DHCP 服务　启用

IP 地址租用期　120 分钟

首选域名服务器 202.104.81.245

备用域名服务器 202.96.128.68

DHCP 地址池　起始地址 10.11.100.2 地址数 253

掩码 255.255.255.0　缺省路由　10.11.100.1

- 用户名和密码

管理用户　admin / password

普通用户　manager / password

- Radius 管理

Radius 服务　启用

Radius 客户端　不启用

- WEB 认证控制

WEB 认证用户首次访问的 URL　about:blank

认证用户 Keep-alive 间隔　1200 秒

认证用户 Keep-alive 超时　3600 秒

认证用户 idle-timeout 检测　启用

认证用户 idle-timeout　15 分钟

认证用户 idle-timeout 流量上限　3KB

- 路由

缺省路由　192.168.0.1

- NAT 规则

Direct　WAN　10.11.100.0/24　192.168.0.126/32　NAPT

Direct　WAN　10.11.100.0/24　192.168.0.126/32

Direct　WAN　192.168.1.0/24　192.168.0.126/32　NAPT

Direct　WAN　192.168.1.0/24　192.168.0.126/32